IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation,	)	
Plaintiff,	)	
v.	)	C. A. No.: 04-1199 (SLR)
INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware Corporation,	)	
Defendants.		

DECLARATION OF STUART STANIFORD

I, Stuart Staniford, hereby declare as follows:

1. I have been retained by counsel for Internet Security Systems, Inc., a Delaware Corporation, and Internet Security Systems, Inc., a Georgia Corporation as an expert witness in this action. If called to testify as to the truth of the matters stated herein, I could and would do so competently.

2. I was educated initially as a theoretical physicist, first in England, and then obtaining a PhD in Physics from the University of California at Davis in 1993. I found myself most passionate about computer work, and decided to obtain a Masters of Science in Computer Science.

3. I joined the computer intrusion detection group at UC Davis in 1994. This was the group that invented network intrusion detection in the late 1980s. I began in that group as a graduate student, and left in 1997 as an assistant adjunct professor.

4. While at UC Davis I initially worked on methods to track hackers back to their true locations. Then I led a team of other researchers and students that developed GrIDS, the first intrusion detection system aimed at wide area networks that used a multi-layer hierarchy. Next I was asked by DARPA (the Defense Advanced Research Projects Agency) to lead the development of the Common Intrusion Detection Framework (CIDF) – an effort to get all the intrusion detection research systems funded by DARPA to interoperate together.

5. In 1997, I founded my own company Silicon Defense, with the intention of doing further DARPA research. During that time, I became co-chair of an Internet Engineering Task Force working group that developed an intended standard for intrusion detection research (IDWG). I then went on in recent years to work primarily on the problem of computer worm spread, and the quantitative performance of algorithms for preventing worm spread. I currently make my living as an independent consultant working primarily in these areas.

6. My research papers on computer intrusion detection, worm spread, and worm containment have been cited by other researchers over 1200 times according to scholar.google.com in March 2006.

7. A summary of my professional experience and publications are attached as Exhibit A.

8. During the course of July and August, 1997, I recall that GrIDS was deployed on a number of computers within the Computer Science Department of UC Davis. This involved deployment on, to the best of my recollection, at least 30 computers

in at least five different laboratories within the department. (The laboratories were rooms that held typically 5-10 graduate students with their equipment).

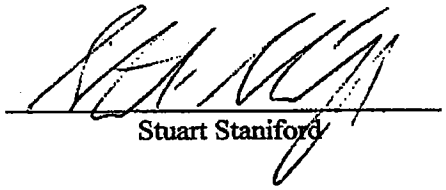
9. The aforementioned departmental GrIDS deployment involved extensive negotiations with the faculty and support staff of the department explaining to them the operation of GrIDS, meeting their concerns over potential privacy issues in monitoring of departmental computers by the GrIDS team, and developing a policy covering this operation. I was involved in these discussions and made the first draft of the policy.

10. I recollect that all faculty, staff, and graduate students of the department were informed of the GrIDS deployment via use of the "csdiv" email alias. The GrIDS deployment, the general nature of GrIDS, and the policies covering its deployment were not secret and no restrictions were placed on discussion of them by any member of the department.

11. Four email messages are attached as Exhibit B. I believe these to be genuine and accurate copies of emails sent on the dates within them, to and from the persons in the email headers. They provide additional details of the policy and communications described above.

12. I declare that all statements made herein are of my own knowledge and are true.

Dated: June 30 2006



Stuart Staniford

EXHIBIT A

Stuart Staniford, PhD

690 Hearst Ave,
San Francisco, CA 94112
stuartstaniford@sbcglobal.net
(415) 239-2090

Summary

I am a researcher, inventor, and entrepreneur. My scientific interests include computer worm propagation, defenses against computer worms, and issues surrounding energy security. My research has led to over one thousand academic citations to date, as well as media coverage in national magazines and newspapers. I also have business and management experience as an entrepreneur in the information security industry.

Work Experience

Invicta Consulting. President, Jan 2005 - Present

Solo Consultant. Clients presently include:

- ***King and Spalding/ISS.*** Jan 2005 - present. Consult on technical issues related to pending intellectual property litigation (SRI is suing ISS for patent infringement).
- ***Nevis Networks.*** Jul 2005 - present. Consult on maintenance issues arising in systems that I designed, help with patent filings arising from my time there as an employee, review security algorithms, help with product testing, and write white papers. *As of this writing, patent filing role has concluded.*
- ***FireEye.*** Mar 2006 - present. Review algorithms, provide third party validation of effectiveness of system. *NB. As of this writing, engagement is verbally agreed but contract is still to be signed. Thus client engagement is likely but not certain.*

The Oil Drum. Editor, September 2005 – Present

Wrote hundreds of blog posts for this popular website exploring the scientific issues surrounding peak oil, economic response to oil shocks, and climate change.

Nevis Networks. Principal Scientist, April 2004 – July 2005

Architected a very high-speed event correlation system and the traffic anomaly subsystem for this startup developing 10Gbps network security solutions for the ethernet edge of internal enterprise networks. These systems resulted in four patents including a novel multi-dimensional external memory algorithm for storing log-records on disk at very high speeds. Designed portions of the product's graphical user interface. Worked extensively with engineering teams in Pune, India and Santa Clara, California implementing my designs.

Silicon Defense. Founder and President, 1998 - 2004

Managed 23 staff performing a mixture of government contract research and commercial product development. Obtained ten research contracts for the company up to $2.3m in size, working for four different DARPA program managers. Performed and published research into intrusion detection, intrusion correlation, and especially worms. Work was covered in Business Week, Federal Computer Week, PC World, Network World, American Banker, and others. Spoke to a variety of audiences on research and risks in cyberspace. Coauthored patent application on invention of worm containment.

Wrote business plan for the company and raised angel capital. Sold commercial products into Fortune 500 accounts (company gained over 50 commercial customers during my tenure). Had profit and loss responsibility for a $1.75m operation. Extensive experience interacting with press, analyst, and investment communities. Also served on a number of program committees and led two standards groups.

After five years of 100%+ growth out of cashflow alone, company was obliged to file bankruptcy due to DARPA's decision to classify further research in the information security area.

UC Davis. Researcher, 1994 – 1997, and Assistant Adjunct Professor, 1997 - 1999

Founded and cochaired the working group that developed the Common Intrusion Detection Framework at the request of DARPA. This involved working with a team of over a hundred researchers and developers from a wide variety of companies and organizations. Led a team of ten researchers and students building a large, distributed, intrusion-detection system (GrIDS). Performed research in new statistical techniques to help in tracing intruders across the Internet. Presented work at conferences and to funding agencies. Wrote successful funding proposals and published papers on work.

Education

M.S. (Computer Science). March 1995. University of California at Davis. Advisor: Prof. Karl Levitt

Ph.D. (Physics) June 1993. University of California at Davis. Awarded fellowships for three years consecutively.

M.S. (Physics) June 1990. University of California, Davis.

B.Sc. (Mathematical Physics) June 1988. University of Sussex, UK. First Class Honors.

Refereed Publications

S. Staniford, D. Moore, N. Weaver, and V. Paxson, *The Top Speed of Flash Worms.* Proceeding of the ACM Workshop on Rapid Malcode (WORM), 2004

N. Weaver, D. Ellis, S. Staniford, and V. Paxson, *Worms vs Perimeters – The Case for Hard-LANS.* Proceedings of Hot Interconnects, 2004

N. Weaver, V. Paxson, and S. Staniford, *Very Fast Scanning Worm Containment.* Proceedings of USENIX Security, 2004

S. Staniford. *Containment of Scanning Worms in Enterprise Networks.* To appear in the Journal of Computer Security.

N. Weaver, V. Paxson, S. Staniford, and R. Cunningham *A Taxonomy of Computer Worms.* Proceedings of the ACM Workshop on Rapid Malcode (WORM). Washington D.C. October, 2003.

D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, *Inside the Slammer Worm*, IEEE Security and Privacy, July/August 2003.

S. Staniford, J. Hoagland and J. McAlerney. *Practical Automated Detection of Stealthy Portscans.* Journal of Computer Security. Vol 10, Issue 1/2, 2002.

S. Staniford, V. Paxson, and N. Weaver *How to Own the Internet in Your Spare Time,* Proceedings of the 11th USENIX Security Symposium 2002.

D. Donoho, A. Flesia, U. Shankar, V. Paxson, J. Coit, and S. Staniford, *Multiscale Stepping-Stone Detection: Detecting Pairs of Jittered Interactive Streams by Exploiting Maximum Tolerable Delay*, Proc. RAID 2002.

J. Hoagland, and S. Staniford, *Viewing IDS alerts: Lessons from SnortSnarf.* Proceedings of DISCEX II, Anaheim, June 2001.

J. Coit, S. Staniford, and J. McAlerney. *Towards Faster Pattern Matching for Intrusion Detection: Exceeding the Speed of Snort.* Proceedings of DISCEX II, Anaheim, June 2001.

R. Feiertag, S. Rho, L. Benzinger, S. Wu, T. Redmond, C. Zhang, K. Levitt, D. Peticolas, M. Heckman, S. Staniford-Chen, and J. McAlerney, *Intrusion Detection Inter-component Adaptive Negotiation.* Computer Networks. 2000.

S. Staniford, J. Hoagland and J. McAlerney. *Practical Automated Detection of Stealthy Portscans.* Proceedings of the ACM CCS IDS Workshop,November 1, 2000. Athens, Greece.

R. Feiertag, S. Rho, L. Benzinger, S. Wu, T. Redmond, C. Zhang, K. Levitt, D. Peticolas, M. Heckman, S. Staniford-Chen, and J. McAlerney,. ***et al.*** *Intrusion Detection Inter-Component Adaptive Negotiation.* Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID 99), Lafayette, Indiana; September, 1999.

S. Staniford-Chen, B. Tung, and D. Schnackenberg,. *The Common Intrusion Detection Framework (CIDF).* Proceedings of 1998 Information Survivability Workshop – ISW'98, Orland, Florida; October, 1998.

S. Staniford-Chen, S. ***et al*** *GrIDS: A Graph-Based Intrusion Detection System for Large Networks.* Proceedings of the 19th NISSC, Baltimore, 1996.

S. Staniford-Chen, and L.T. Heberlein, *Holding Intruders Accountable on the Internet.* Proceedings of the 1995 IEEE Symposium on Security and Privacy, Oakland, CA. 1995.

J. Kiskis and S. Staniford-Chen, *Universal Amplitude Ratios and Functions for the SU(2), Finite-Temperature Phase Transition.* In Axen, D., Bryman, D., and Comyn, N. (eds) Vancouver Meeting. Particles and Fields '91. p 821. World Scientific. 1992.

Published Reports and Theses

N. Weaver, V. Paxson, and S. Staniford, *The Worst Case Worm.* Silicon Defense Technical Report. August 2003.

S. Staniford and C. Kahn, *Worm Containment on the Internal Network.* Silicon Defense Technical White Paper. March 2003

N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, *Large Scale Malicious Code: A Research Agenda.* Silicon Defense Technical Report, Dec 2002.

B. Tung, et al. The Common Intrusion Detection Framework Specification. Nov 2001.

S. Staniford, O.S. Saydjari, and K. Williams *The US is Not Safe in a Cyberwar.* Paper presented to Department of Defense and National Security Council executives. May 2001. 2nd Edition.

S. Staniford, O.S. Saydjari, and K. Williams *The US is Not Safe in a Cyberwar.* Paper presented to DARPA. Sep 2000.

S. Cheung, S. ***et al*** *The Design of GrIDS: A Graph-Based Intrusion Detection System*. UCD Technical Report CSE-99-2, January, 1999.

S. Staniford-Chen, *Distributed Tracing of Intruders*. Master's Thesis, University of California at Davis. 1995.

S. Staniford-Chen, Finite Size Scaling and the Universality Class of SU(2) Lattice Gauge Theory. PhD Thesis, University of California at Davis. 1993.

S. Staniford-Chen, *Finite Size Scaling of Probability Distributions in SU(2) Lattice Gauge Theory and Phi^4 Field Theory* . Preprint UCD-92-17, University of California at Davis. 1992.

Patent Filings

S. Staniford and M. Bakshi, *A System and Method for Selecting Memory Locations for Overwrite.* Filed January 23rd, 2006

S. Staniford ***et al,*** *A System and Method for Aggregating and Consolidating Security Event Data.* Filed November 26th, 2005

S. Staniford and T. Mustafa, *A System and Method for Deprioritizing and Presenting Data.* Filed November 4th, 2005

S. Staniford and P. Sobel. *System and method for storing multi-dimensional network and security event data.* Filed October 14th, 2005

S. Staniford, C. Kahn, N. Weaver, C. Coit, and R. Jonkman , *Method and system for reducing the rate of infection of a communications network by a software worm.* Filed December 6th, 2002. Filing serial number: 313623.

Software Systems

CounterMalice was the first automated worm containment system in the world capable of containing zero-day worms, and became a commercial product. It operates by dividing a network into cells, recognizing wormlike behavior, and suppressing spread of a worm from one cell to another. CounterMalice was developed with Cliff Kahn, Nick Weaver, Jason Coit, Roel Jonkman, Joe McAlerney, and Dan Watson. My role was providing the initial vision, developing quantitative methods for tuning the system such that its performance against worms could be engineered in advance, and coding portions of the user interface.

Spice was the first system capable of detecting stealthy portscans from multiple sources using simulated annealing to correlate disparate events. It became part of a commercial product (CounterStealth). Spice was developed with James Hoagland and Dan Watson. My role was initial vision, much of the design, and techniques for validating its performance.

Spade was a network anomaly detection system (used as an input to Spice). It became well known and gained widespread operational use when it was incorporated as a plug-in into the open-source GPL intrusion detection system Snort. Spade was developed with James Hoagland. My role was the basic idea and much of the design.

Snortsnarf was an open-source alert viewer for Snort, that was innovative in systematically taking account of the possibility of attackers deliberately targeting the user interface screen real-estate. Snortsnarf gained widespread operational use at sites generating large volumes of Snort alerts, and was the main user interface for intrusion detection at the 2002 Winter Olympics. Snortsnarf was developed with James Hoagland. My role was to build the first version of the system, and provide design input during ongoing maintenance and extension.

GrIDS was the first intrusion detection/correlation system capable of correlating alerts hierarchically to infer the presence of large scale automated attacks throughout a network (including scans and worms). The system could handle a wide variety of inference tasks through a set of rules that assembled activity into distributed graphs which the system reasoned about. The inference hierarchy could by dynamically rearranged via a drag-and-drop UI. GrIDS was developed with Mark Dillinger, James Hoagland, Chris Wee, Dan Zerkle, Rich Crawford, Steven Templeton, Stephen Cheung, and Karl Levitt. My role was that of team leader/group facilitator, contributor to the design of the inference mechanism and hierarchy, and implementer of the components that supported the rearrangable hierarchy. GriDS was tested in a medium-sized deployment at UC Davis.

Funding Obtained

Network Associates (subcontract under DARPA contract). *Intrusion Detection InterComponent Adaptive Negotiation.* $100k (1998-1999)

University of California, Davis (subcontract under DARPA contract). Global Guard: A Protection Architecture for Survivability of Large Scale, High-Confidence Information Networks. $90k (1999-2000)

The Boeing Company (subcontract under DARPA contract). Multi-Community Cyber Defense. $480k (1999-2002)

EMC Corp. Explorations of Randomness in Hard Disk Rotation Times. $32k (1999-2000)

WetStone Technologies (subcontract under DARPA contract). NetFlare IDWG subcontract. 2000-2001

DARPA Internet Trap-and-Trace. $2.3m (2000-2003). With Felix Wu (UC Davis) and Vern Paxson, ICIR.

US Air Force, Rome Labs. IDS Correlation Using IDWG. $50k (2000-2001)

US Air Force, Rome Labs. IA-INTER-OP IETF IDWG. $145k (2001-2003). Co-PI with Joseph Betser

Northrop Grumman (subcontract under DARPA contract). International Coalition Exercises. $203k (2002-2003)

BBN Technologies (subcontract under DARPA contract). Information Assurance Operational Experimentation. $500k (2002-2003)

Service

Program committee member of the **ACM Workshop on Rapid Malcode (WORM)**. 2005

Advisory board member for the **Collaborative Center for Internet Epidemiology and Defenses**. 2004-present

General chair and program committee member of the **ACM Workshop on Rapid Malcode (WORM)**. 2003

Co-organizer of the DIMACS Workshop on Large Scale Wttacks, 2003.

Served on the program committee of the Symposium on **Recent Advances in Intrusion Detection (RAID)** from 1999-2003.

Member of the **Mitre CVE Editorial Board**. This group developed a standard naming system for computer vulnerabilities. (1999-2002, now emeritus member)

Founded and cochaired the **IETF working group IDWG** (1999-2004). This working group has almost completed work on a set of documents to allow common reporting by disparate intrusion detection systems. These should become RFCs shortly.

Founded and chaired the **Common Intrusion Detection Framework** working group, at the request of DARPA (1998-2000). This group was responsible for developing a standard for

all DARPA-funded intrusion detection researchers to build their systems to in order to allow inter-operation.

Invited Presentations

Usenix Security, 2004. *Military Strategy in Cyberspace.* San Diego, August 2004.

University of California, Davis. *Worms and Worm Containment.* Seminar at Computer Science Department, Feb 2003.

John Moores University Computer Science Department. *Worms and Worm Containment.* Seminar at Computer Science Department, Dec 2003.

DIMACS Workshop on Large Scale Attacks. *Introduction to Worms and Worm Containment.* Oct 2003.

The Forum on Information Warfare. Future *Technologies of Cyberwar Operations.* November 2003

Microsoft Corporation. *Worms and CounterMalice – presentation to the Security Business Unit.* Sep 2003.

Government Communications Conference. *Cyber-Weapons of Mass Destruction.* Invited Keynote Presentation. July 2003.

Annual Computer Security Applications Conference. *Defeating Worms.* Invited panel presentation. Dec 2002.

AT&T. *Worms and Anti-worm devices.* Invited presentation to security group. Sep 2002.

National Security Agency. *Worms and Traceback.* Invited presentation to technical groups. Aug 2002.

UC Berkeley. *Military Strategy in CyberSpace.* Invited lecture as part of a special series of lectures on critical infrastructure protection. Mar 2002.

Ground Systems Architectures Workshop. *CyberSpace risks to Ground Systems.* Invited presentation on risks to satellite ground systems due to dependence on the Internet. Mar 2002.

Annual Computer Security Applications Conference. *IDWG Progress Report* – invited panel presentation. Dec 2001.

ACM Conference on Computer Security. *Detecting Distributed Portscans.* Tutorial as part of joint tutorial with Vern Paxson on Intrusion Correlation. Nov 2001.

RAID Symposium. *State of Intrusion Detection*. Invited Panel Presentation. Oct 2001.

National Security Telecommunications Advisory Council. *The US is not safe in a cyberwar*. Joint work with O. Sami Saydjari (presenting) and Ken Williams. June 2001.

SRI Workshop on Adversary Characterization. *Cyberwar and Strategy – some lessons from history*. Aug 2001.

SANS National Conference. *Viewing Snort Alerts with Snortsnarf*. May 2001.

CanSecWest. *Spade and Spice*. Mar 2001.

RAID Symposium. *IDWG: Progress towards an open IDS alert standard*. October 2000.

National Security Council. *Presentation to members of the NSC staff on future risks from cyber attacks on US*. Sep 2000.

RAID Symposium. *IDS Standards – Lessons Learned to Date*. September 1999.

CIO Council, Monterey Meeting. *Standardizing IDS Alerts*. March 1999.

White House Workshop on Cybersecurity Research. *Standardizing IDS Alarms*. February 1999.

Selected Press Coverage of Work

Stuart Staniford's work has been featured in several dozen news stories in the major media and computer technical publications. A small sample include:

Business Week To Trap a Superworm
http://www.businessweek.com/technology/content/feb2003/tc20030225_4104_tc047.htm
The Slammer worm's ability to spread so rapidly adds a frightfully new dimension to the species. Does Stuart Staniford have the cure?

PC World Dawn of the Superworm,
http://www.pcworld.com/news/article/0,aid,110014,00.asp

ComputerWorld Study: Slammer was fastest spreading worm yet,
http://www.idg.com.hk/cw/readstory.asp?aid=20030205005

The Independent Internet worm took 10 minutes to create global chaos,
http://news.independent.co.uk/digital/news/story.jsp?story=375374

EXHIBIT B

Date: Wed, 16 Jul 97 15:53:33 -0700
From: Stuart Staniford-Chen <stanifor@jaya.cs.ucdavis.edu>
To: martel@toadflax.cs.ucdavis.edu, olsson@toadflax.cs.ucdavis.edu,
fulton@toadflax.cs.ucdavis.edu, rowe@toadflax.cs.ucdavis.edu,
csprog@toadflax.cs.ucdavis.edu
Subject: Third and final grids policy proposal
Cc: grids@cs.ucdavis.edu
Reply-To: stanifor@toadflax.cs.ucdavis.edu

After the meeting that Jeff and I had with concerned faculty and staff this afternoon, this is the third revised version of the GrIDS policy. This one is assumed to be final unless people feel that it doesn't capture correctly what we agreed to this afternoon.

Policy for GrIDS deployment in the Research Wing.

This policy is in effect for the short term (until the ITC is able to formulate a long term policy.)

The GrIDS operators may deploy GrIDS on computers in the research wing but not belonging to the computer security group, only under the following conditions.

1. The version of GrIDS used will monitor computer systems and networks only via publically available Unix commands (ie, commands which come with the operating system and do not require root privilege to run) and via a network monitor program. No network segments containing faculty or staff workstations will be monitored. The network monitor program will not output any human-generated information (such as contents or subject lines of email, passwords, or contents of files). It will only record or output summary data about network traffic to include such things as the time a connection was made, the source and destination address and port,
protocol information such as NFS filehandles, TCP sequence numbers, usernames, etc. GrIDS will not record or display any data concerning any traffic between two machines where neither machine is covered by GrIDS.

2. GrIDS will be used only for the purpose of detecting intrusions or doing research in intrusion detection. The operators of the system will not use it with the intent of gathering information about individual users. Any information about activities of individual users that should chance to come to the attention of the operators will not be revealed to anyone else except in two cases:
   A. the operators believe in good faith that that activity is in violation of the law or of the UC Davis acceptable use policy. In this case, they may only inform departmental system administrators, and they are encouraged to do that.
   B. the information is revealed for the purpose of illustration or reporting of research results and is in such a form that it cannot be determined who undertook the activity.

Any accounts given to the operators for the purpose of installing and using GrIDS will not be used for other purposes without written permission.

3. For each machine covered by GrIDS, prior written permission must have been obtained from a faculty member responsible for that machine and from the departmental system administrators. All users with accounts on that machine must have been notified in writing of the GrIDS monitoring. Such notification must include a copy of this document. If they object to the monitoring, they shall have the right to be excluded from it. The GrIDS operators shall take such steps to avoid monitoring them as necessary to meet the objecting user's requirements. In addition, a general notice informing the computer science department of this project will be sent to the csdiv alias and posted on the doors

of affected research labs.

4. The only personnel authorized to operate the GrIDS software (on machines other than those of the computer security group) are Jeff Rowe, Rick Crawford, and Stuart Staniford-Chen. The operators may receive help from other members of the GrIDS team in installing the software, but must ensure that the version used is in compliance with this policy. Other people may not run the software or monitor its output. Dr Rowe will generally be doing the day-to-day work with the system. Ultimate responsibility for ensuring the operation of the system in accordance with this policy lies with Prof. Staniford-Chen.

Jeff Rowe	rowe@cs.ucdavis.edu	2-1287
Rick Crawford	crawford@cs.ucdavis.edu	4-8380
Stuart Staniford-Chen	stanifor@cs.ucdavis.edu	2-1287, 707-442-5088

The mail alias monitor@cs.ucdavis.edu reaches all GrIDS operators together with departmental personnel concerned about the operation of GrIDS.

5. Anyone having a concern about the operation of GrIDS is encouraged to raise the issue with the operators by sending mail to the monitor@cs.ucdavis.edu mailing list. If the concern cannot be addressed this way, it may be taken to the department chair. The department chair can impose additional conditions or suspend the operation of GrIDS as he sees fit. When the chair asks for suspension, he will notify the operators in writing and they will cease running of GrIDS as soon as they are at work and available to do so.

6. Where written communication to a person is required by this policy, email to any account belonging to that person is assumed to be an adequate method. Copies of all communications covered by this policy will be kept by the grids operators.

From rowe@erebus.cs.ucdavis.edu Thu Jul 17 18:05:11 1997
Received: from erebus (erebus.cs.ucdavis.edu) by toadflax.cs.ucdavis.edu (4.1/UCD.CS.2.6)
id AA13060; Thu, 17 Jul 97 18:05:07 PDT
Received: from erebus.cs.ucdavis.edu by erebus (SMI-8.6/UCDCS.SECLAB.Solaris2-2.1)
id SAA26611; Thu, 17 Jul 1997 18:05:07 -0700
Message-Id: <199707180105.SAA26611@erebus>
X-Mailer: exmh version 1.6.2 7/18/95
To: vijay@ece.ucdavis.edu, ramu@cs.ucdavis.edu, juej@cs.ucdavis.edu,
vijoy@cs.ucdavis.edu, byrav@cs.ucdavis.edu, iness@cs.ucdavis.edu,
sahasrab@cs.ucdavis.edu
Cc: stanifor@erebus.cs.ucdavis.edu
Subject: Including Network Lab Machines in our Intrusion Detection Demo.
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Date: Thu, 17 Jul 1997 18:04:57 -0700
From: Jeff Rowe <rowe@erebus.cs.ucdavis.edu>

Hi:

My name is Jeff Rowe and I'm a postdoc in the computer security lab.
I work as part of a team which has developed the Graph-based Intrusion
Detection System (GrIDS). After extensive review, the department has
agreed to let us install the GrIDS system on machines in the research
wing for the purposes of research and testing on a larger scale than
we can manage in the security lab alone.

We have solicited help from Profs. Mukherjee and Ghosal and they have agreed to let us use the machines in the Network Lab of which you are a user. In order to keep you informed and to ensure that your rights aren't violated, the department and GrIDS personnel have agreed on a policy covering this deployment. A copy is attached to this message and we encourage you to read it. Perhaps the most important point is that you have the right to opt out being covered by this system. We believe the invasion on your privacy will be minimal, but if you are uncomfortable, please read the policy and follow the suggestion there for opting out.

We are also including an explanation of what GrIDS does to help you make a more informed decision. If at any time you have concerns or need more information, don't hesitate to contact me at rowe@cs.ucdavis.edu or drop in Room 2244 accross the hall and we can talk.

Thanks for your time,

Jeff Rowe.
rowe@cs.ucdavis.edu
Security Lab (Room 2244)
916-752-1287

Background Information about GrIDS.

GrIDS is designed to detect automated attacks on large networks. It detects these attacks by putting together patterns of network events into graphs. Analysis of these graphs provides evidence that someone might be systematically searching or propogating software through the network.

To build the graphs, one data source that we use is a network monitor which looks primarily at headers of low-level TCP and UDP packets. To protect the privacy of all users, under no circumstances does GrIDS process user-generated data, neither does it process passwords. This information is discarded at the source. For only two protocols: rsh and NFS, are higher level protocols accessed, specifically to determine the user id and rsh command issued. As a general rule, the information monitored by GrIDS is freely available using standard Unix commands (netstat, lastcomm, ps, etc).

As an example, the lowest level data from our monitor for a typical TCP connection is shown below.

```
digraph sniffer { "erebus.cs.ucdavis.edu" -> "kanab.cs.ucdavis.edu"
[ ctype="unknown", prot="tcp", sport=50299, dport=663, timestamp="17:01:19",
  time=868406479, seq=2192100389, stage="START", status="SUCC",
  id="erebus.cs.ucdavis.edukanab.cs.ucdavis.edu50299663868406479 2192100389"
 ] ; }
```

Note that the data fields of interest are the sending and receiving hosts and ports, along with the protocol, time and status. Under normal operating conditions this is piped directly into GrIDS and not seen by the operator. We attempt to minimize the data finally presented to the operator to guarantee the privacy of all users on the system.

The impact upon machine resources should be fairly minimal with only one and occasionally two processes running per machine. These processes consume very little cpu time (<1%) and memory requirements are typically several Mbytes; about the equivalant of two additional xterm windows.

Policy for GrIDS deployment in the Research Wing.

This policy is in effect for the short term (until the ITC is able to formulate a long term policy.)

The GrIDS operators may deploy GrIDS on computers in the research wing but not belonging to the computer security group, only under the following conditions.

1. The version of GrIDS used will monitor computer systems and networks only via publically available Unix commands (ie, commands which come with the operating system and do not require root privilege to run) and via a network monitor program. No network segments containing faculty or staff workstations will be monitored. The network monitor program will not output any human-generated information (such as contents or subject lines of email, passwords, or contents of files). It will only record or output summary data about network traffic to include such things as the time a connection was made, the source and destination address and port, protocol information such as NFS filehandles, TCP sequence numbers, usernames, etc. GrIDS will not record or display any data concerning any traffic between two machines where neither machine is covered by GrIDS.

2. GrIDS will be used only for the purpose of detecting intrusions or doing research in intrusion detection. The operators of the system will not use it with the intent of gathering information about individual users. Any information about activities of individual users that should chance to come to the attention of the operators will not be revealed to anyone else except in two cases:

   A. the operators believe in good faith that that activity is in violation of the law or of the UC Davis acceptable use policy. In this case, they may only inform departmental system administrators, and they are encouraged to do that.
   B. the information is revealed for the purpose of illustration or reporting of research results and is in such a form that it cannot be determined who undertook the activity.

Any accounts given to the operators for the purpose of installing and using GrIDS will not be used for other purposes without written permission.

3. For each machine covered by GrIDS, prior written permission must have been obtained from a faculty member responsible for that machine and from the departmental system administrators. All users with accounts on that machine must have been notified in writing of the GrIDS monitoring. Such notification must include a copy of this document. If they object to the monitoring, they shall have the right to be excluded from it. The GrIDS operators shall take such steps to avoid monitoring them as necessary to meet the objecting user's requirements. In addition, a general notice informing the computer science department of this project will be sent to the csdiv alias and posted on the doors of affected research labs.

4. The only personnel authorized to operate the GrIDS software (on machines other than those of the computer security group) are Jeff Rowe, Rick Crawford, and Stuart Staniford-Chen. The operators may receive help from other members of the GrIDS team in installing the software, but must ensure that the version used is in compliance with this policy. Other people may not run the software or monitor its output. Dr Rowe will

generally be doing the day-to-day work with the system. Ultimate responsibility for ensuring the operation of the system in accordance with this policy lies with Prof. Staniford-Chen.

Jeff Rowe	rowe@cs.ucdavis.edu	2-1287
Rick Crawford	crawford@cs.ucdavis.edu	4-8380
Stuart Staniford-Chen	stanifor@cs.ucdavis.edu	2-1287, 707-442-5088

The mail alias monitor@cs.ucdavis.edu reaches all GrIDS operators together with departmental personnel concerned about the operation of GrIDS.

5. Anyone having a concern about the operation of GrIDS is encouraged to raise the issue with the operators by sending mail to the monitor@cs.ucdavis.edu mailing list. If the concern cannot be addressed this way, it may be taken to the department chair. The department chair can impose additional conditions or suspend the operation of GrIDS as he sees fit. When the chair asks for suspension, he will notify the operators in writing and they will cease running of GrIDS as soon as they are at work and available to do so.

6. Where written communication to a person is required by this policy, email to any account belonging to that person is assumed to be an adequate method. Copies of all communications covered by this policy will be kept by the grids operators.

From rowe@erebus.cs.ucdavis.edu Thu Jul 17 18:17:38 1997
Received: from erebus (erebus.cs.ucdavis.edu) by toadflax.cs.ucdavis.edu (4.1/UCD.CS.2.6)
id AA13196; Thu, 17 Jul 97 18:17:35 PDT
Received: from erebus.cs.ucdavis.edu by erebus (SMI-8.6/UCDCS.SECLAB.Solaris2-2.1)
id SAA26709; Thu, 17 Jul 1997 18:17:35 -0700
Message-Id: <199707180117.SAA26709@erebus>
X-Mailer: exmh version 1.6.2 7/18/95
To: prieditis@cs.ucdavis.edu
Cc: stanifor@erebus.cs.ucdavis.edu
Subject: Permission to use your machines in the AI Lab.
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Date: Thu, 17 Jul 1997 18:17:35 -0700
From: Jeff Rowe <rowe@erebus.cs.ucdavis.edu>

Hello Prof. Prieditis,

We probably haven't met, but I work with Karl Levitt and Stuart Staniford-Chen as a post-doc in the Security Lab. I work as part of a team which has developed the Graph-based Intrusion Detection System (GrIDS). After extensive review, the department has agreed to let us install the GrIDS system on machines in the research wing for the purposes of research and testing on a larger scale than we can manage in the security lab alone.

We would very much like to include machines from your lab (Room 2231). In order to ensure that user's rights aren't violated, the department and GrIDS personnel have agreed on a policy covering this deployment. A copy is attached to this message for your reference. Although we believe that the invasion on your user's privacy will be minimal, please notice that we include a provision for them to opt out being covered by this system if they wish.

Also included below is a a brief explanation of what GrIDS does. The impact on machine resources should be fairly minimal with only one and occasionally two processes running per machine. These processes consume very

little cpu time (<1%) and memory requirements are typically several Mbytes; about the equivalant of two additional xterm windows.

If you agree, please reply to me at rowe@cs.ucdavis.edu. We will need an account on your machines: a personal account for myself would be ideal. If the keep3 home disk is mounted, none of your disk resources need be used at all. The inclusion of your machines would be a big boost for our project. If there is a time that we could meet I would be happy to discuss this with you in person and answer any questions that you may have.

Cheers,

Jeff Rowe
rowe@cs.ucdavis.edu
Security Lab (Room 2244)
(916)-752-1287

Background Information about GrIDS.

GrIDS is designed to detect automated attacks on large networks. It detects these attacks by putting together patterns of network events into graphs. Analysis of these graphs provides evidence that someone might be systematically searching or propogating software through the network.

To build the graphs, one data source that we use is a network monitor which looks primarily at headers of low-level TCP and UDP packets. To protect the privacy of all users, under no circumstances does GrIDS process user-generated data, neither does it process passwords. This information is discarded at the source. For only two protocols: rsh and NFS, are higher level protocols accessed, specifically to determine the user id and rsh command issued. As a general rule, the information monitored by GrIDS is freely available using standard Unix commands (netstat, lastcomm, ps, etc).

As an example, the lowest level data from our monitor for a typical TCP connection is shown below.

```
digraph sniffer { "erebus.cs.ucdavis.edu" -> "kanab.cs.ucdavis.edu"
[ ctype="unknown", prot="tcp", sport=50299, dport=663, timestamp="17:01:19",
   time=868406479, seq=2192100389, stage="START", status="SUCC",
  id="erebus.cs.ucdavis.edukanab.cs.ucdavis.edu50299663868406479 2192100389"
] ; }
```

Note that the data fields of interest are the sending and receiving hosts and ports, along with the protocol, time and status. Under normal operating conditions this is piped directly into GrIDS and not seen by the operator. We attempt to minimize the data finally presented to the operator to guarantee the privacy of all users on the system.

The impact upon machine resources should be fairly minimal with only one and occasionally two processes running per machine. These processes consume very little cpu time (<1%) and memory requirements are typically several Mbytes; about the equivalant of two additional xterm windows.

Policy for GrIDS deployment in the Research Wing.

This policy is in effect for the short term (until the Department of Computer Science's Information Technology Committee is able to formulate a long term policy.)

The GrIDS operators may deploy GrIDS on computers in the research wing but not belonging to the computer security group, only under the following conditions.

1. The version of GrIDS used will monitor computer systems and networks only via publically available Unix commands (ie, commands which come with the operating system and do not require root privilege to run) and via a network monitor program. No network segments containing faculty or staff workstations will be monitored. The network monitor program will not output any human-generated information (such as contents or subject lines of email, passwords, or contents of files). It will only record or output summary data about network traffic to include such things as the time a connection was made, the source and destination address and port, protocol information such as NFS filehandles, TCP sequence numbers, usernames, etc. GrIDS will not record or display any data concerning any traffic between two machines where neither machine is covered by GrIDS.

2. GrIDS will be used only for the purpose of detecting intrusions or doing research in intrusion detection. The operators of the system will not use it with the intent of gathering information about individual users. Any information about activities of individual users that should chance to come to the attention of the operators will not be revealed to anyone else except in two cases:

   A. the operators believe in good faith that that activity is in violation of the law or of the UC Davis acceptable use policy. In this case, they may only inform departmental system administrators, and they are encouraged to do that.
   B. the information is revealed for the purpose of illustration or reporting of research results and is in such a form that it cannot be determined who undertook the activity.

Any accounts given to the operators for the purpose of installing and using GrIDS will not be used for other purposes without written permission.

3. For each machine covered by GrIDS, prior written permission must have been obtained from a faculty member responsible for that machine and from the departmental system administrators. All users with accounts on that machine must have been notified in writing of the GrIDS monitoring. Such notification must include a copy of this document. If they object to the monitoring, they shall have the right to be excluded from it. The GrIDS operators shall take such steps to avoid monitoring them as necessary to meet the objecting user's requirements. In addition, a general notice informing the computer science department of this project will be sent to the csdiv alias and posted on the doors of affected research labs.

4. The only personnel authorized to operate the GrIDS software (on machines other than those of the computer security group) are Jeff Rowe, Rick Crawford, and Stuart Staniford-Chen. The operators may receive help from other members of the GrIDS team in installing the software, but must ensure that the version used is in compliance with this policy. Other people may not run the software or monitor its output. Dr Rowe will generally be doing the day-to-day work with the system. Ultimate responsibility for ensuring the operation of the system in accordance with this policy lies with Prof. Staniford-Chen.

Jeff Rowe rowe@cs.ucdavis.edu 2-1287
Rick Crawford crawford@cs.ucdavis.edu 4-8380
Stuart Staniford-Chen stanifor@cs.ucdavis.edu 2-1287, 707-442-5088

The mail alias monitor@cs.ucdavis.edu reaches all GrIDS operators together with departmental personnel concerned about the operation of GrIDS.

5. Anyone having a concern about the operation of GrIDS is encouraged to raise the issue with the operators by sending mail to the monitor@cs.ucdavis.edu mailing list. If the concern cannot be addressed this way, it may be taken to the department chair. The department chair can impose additional conditions or suspend the operation of GrIDS as he sees fit. When the chair asks for suspension, he will notify the operators in writing and they will cease running of GrIDS as soon as they are at work and available to do so.

6. Where written communication to a person is required by this policy, email to any account belonging to that person is assumed to be an adequate method. Copies of all communications covered by this policy will be kept by the grids operators.

From rowe@erebus.cs.ucdavis.edu Fri Jul 18 16:34:35 1997
Received: from erebus (erebus.cs.ucdavis.edu) by toadflax.cs.ucdavis.edu (4.1/UCD.CS.2.6)
id AA01436; Fri, 18 Jul 97 16:34:30 PDT
Received: from erebus.cs.ucdavis.edu by erebus (SMI-8.6/UCDCS.SECLAB.Solaris2-2.1)
id QAA29782; Fri, 18 Jul 1997 16:34:26 -0700
Message-Id: <199707182334.QAA29782@erebus>
X-Mailer: exmh version 1.6.2 7/18/95
To: grids@erebus.cs.ucdavis.edu
Subject: A copy of the required notice to csdiv users. Comments?
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Date: Fri, 18 Jul 1997 16:34:25 -0700
From: Jeff Rowe <rowe@erebus.cs.ucdavis.edu>

Here's a draft of the notice that the deployment policy requires that we send to csdiv. This is to research wing users who aren't necissarily using machines covered by grids. Since we want to make a good impression on this wide group of individuals, I'm running it by GrIDS members for comments/suggestions before distribution.

Cheers,
Jeff Rowe.

Hi:

My name is Jeff Rowe and I'm a postdoc in the computer security lab. I work as part of a team which has developed the Graph-based Intrusion Detection System (GrIDS). After extensive review, the department has agreed to let us install the GrIDS system on machines in the research wing for the purposes of research and testing on a larger scale than we can manage in the security lab alone. We will only be installing this in labs where we have obtained the permission of the P.I. in question,

GrIDS is designed to detect automated attacks on large networks. It detects these attacks by putting together patterns of network events into graphs. To collect network events, we monitor network traffic to and from machines included in our system. To protect the privacy of all users, under no circumstances does GrIDS process user-generated data, neither does it process passwords. As a general rule, the information monitored

by GrIDS is freely available using standard Unix commands (netstat, lastcomm, ps, etc). Although the impact on the privacy of individual users will be slight, we will be specifically contacting everyone who's privacy may be affected with more information.

This message is simply to inform all other computer science users of the situation. If at any time you have concerns or need more information, please contact us at monitor@cs.ucdavis.edu. I have attached a copy of the policy agreed upon by the Department and the GrIDS team covering this deployment for your reference.

Thanks,
Jeff Rowe.

------- End of Forwarded Message

CERTIFICATE OF SERVICE

I hereby certify that on the 30th day of June, 2006, I electronically filed the foregoing document, **DECLARATION OF STUART STANIFORD,** with the Clerk of the Court using CM/ECF which will send notification of such filing to the following:

John F. Horvath, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
Wilmington, DE 19801

Additionally, I hereby certify that on the 30th day of June, 2006, the foregoing document was served via email and by Federal Express on the following non-registered participants:

Howard G. Pollack, Esq.
Michael J. Curley, Esq.
Fish & Richardson
500 Arguello Street, Suite 500
Redwood City, CA 94063
650.839.5070

Holmes Hawkins, III, Esq.
King & Spalding
191 Peachtree Street
Atlanta, GA 30303
404.572.4600

Theresa Moehlman, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
212.556.2100

/s/ Richard K. Herrmann
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
(302) 888-6800
rherrmann@morrisjames.com

Counsel for Symantec Corporation